from a Federal department or agency, the same written notice to the prospective bidder and end-user, and this notice also will contain a statement of the legal and factual basis for the refusal of certification. The prospective bidder and end-user may, within thirty calendar days of receipt of notification of the refusal, submit written comments or written objections to the Administrator's refusal. At the same time, the prospective bidder and end-user also may provide supporting documentation to contest the Administrator's refusal. If such written comments or written objections raise issues regarding any finding of fact or conclusion of law upon which the refusal is based, the Administrator will reconsider the refusal of the proposed sale in light of the written comments or written objections filed. Thereafter, within a reasonable time, the Administrator will withdraw or affirm the original refusal of certification as he determines appropriate. The Administrator will provide written reasons for any affirmation of the original refusal. Such affirmation of the original refusal will constitute a final decision for purposes of judicial review under 21 U.S.C. 877.

(f) If the Administrator determines there is reasonable cause to believe that an existing certification should be withdrawn, DEA will provide written notice to the head of a Federal department or agency of such withdrawal under the authority of 21 U.S.C. 890. DEA also will provide, within fifteen calendar days of withdrawal of an existing certification, the same written notice to the bidder and end-user, and this notice also will contain a statement of the legal and factual basis for the withdrawal. The bidder and end-user may, within thirty calendar days of receipt of notification of the withdrawal of the existing certification, submit written comments or written objections to the Administrator's withdrawal. At the same time, the bidder and end-user also may provide supporting documentation to contest the Administrator's withdrawal. If such written comments or written objections raise issues regarding any finding of fact or conclusion of law upon which the withdrawal of the existing certification is based, the Administrator will reconsider the withdrawal of the existing certification in light of the written comments or written objections filed. Thereafter, within a reasonable time, the Administrator will withdraw or affirm the original withdrawal of the existing certification as he determines appropriate. The Administrator will provide written reasons for any affirmation of the original withdrawal of the existing certification. Such affirmation of the original withdrawal of the existing certification will constitute a final decision for purposes of judicial review under 21 U.S.C. 877.

[68 FR 62737, Nov. 6, 2003]

PART 1311—DIGITAL CERTIFICATES

Subpart A—General

Sec.
1311.01 Scope.
1311.02 Definitions.
1311.05 Standards for technologies for electronic transmission of orders.
1311.08 Incorporation by reference.

Subpart B—Obtaining and Using Digital Certificates for Electronic Orders

1311.10 Eligibility to obtain a CSOS digital certificate.
1311.15 Limitations on CSOS digital certificates.
1311.20 Coordinators for CSOS digital certificate holders.
1311.25 Requirements for obtaining a CSOS digital certificate.
1311.30 Requirements for storing and using a private key for digitally signing orders.
1311.35 Number of CSOS digital certificates needed.
1311.40 Renewal of CSOS digital certificates.
1311.45 Requirements for registrants that allow powers of attorney to obtain CSOS digital certificates under their DEA registration.
1311.50 Requirements for recipients of digitally signed orders.
1311.55 Requirements for systems used to process digitally signed orders.
1311.60 Recordkeeping.

AUTHORITY: 21 U.S.C. 821, 828, 829, 871(b), 958(e), 965, unless otherwise noted.

SOURCE: 70 FR 16915, Apr. 1, 2005, unless otherwise noted.

Subpart A—General

§ 1311.01 Scope.

This part sets forth the rules governing the use of digital signatures and the protection of private keys by registrants.

§ 1311.02 Definitions.

For the purposes of this chapter:

Biometric authentication means authentication based on measurement of the individual's physical features or repeatable actions where those features or actions are both unique to the individual and measurable.

Cache means to download and store information on a local server or hard drive.

Certificate Policy means a named set of rules that sets forth the applicability of the specific digital certificate to a particular community or class of application with common security requirements.

Certificate Revocation List (CRL) means a list of revoked, but unexpired certificates issued by a Certification Authority.

Certification Authority (CA) means an organization that is responsible for verifying the identity of applicants, authorizing and issuing a digital certificate, maintaining a directory of public keys, and maintaining a Certificate Revocation List.

CSOS means controlled substance ordering system.

Digital certificate means a data record that, at a minimum:

(1) Identifies the certification authority issuing it;

(2) Names or otherwise identifies the certificate holder;

(3) Contains a public key that corresponds to a private key under the sole control of the certificate holder;

(4) Identifies the operational period; and

(5) Contains a serial number and is digitally signed by the Certification Authority issuing it.

Digital signature means a record created when a file is algorithmically transformed into a fixed length digest that is then encrypted using an asymmetric cryptographic private key associated with a digital certificate. The combination of the encryption and algorithm transformation ensure that the signer's identity and the integrity of the file can be confirmed.

Electronic signature means a method of signing an electronic message that identifies a particular person as the source of the message and indicates the person's approval of the information contained in the message.

FIPS means Federal Information Processing Standards. These Federal standards, as incorporated by reference in § 1311.08, prescribe specific performance requirements, practices, formats, communications protocols, etc., for hardware, software, data, etc.

FIPS 140–2, as incorporated by reference in § 1311.08, means a Federal standard for security requirements for cryptographic modules.

FIPS 180–2, as incorporated by reference in § 1311.08, means a Federal secure hash standard.

FIPS 186–2, as incorporated by reference in § 1311.08, means a Federal standard for applications used to generate and rely upon digital signatures.

Key pair means two mathematically related keys having the properties that:

(1) One key can be used to encrypt a message that can only be decrypted using the other key; and

(2) Even knowing one key, it is computationally infeasible to discover the other key.

NIST means the National Institute of Standards and Technology.

Private key means the key of a key pair that is used to create a digital signature.

Public key means the key of a key pair that is used to verify a digital signature. The public key is made available to anyone who will receive digitally signed messages from the holder of the key pair.

Public Key Infrastructure (PKI) means a structure under which a Certification Authority verifies the identity of applicants, issues, renews, and revokes digital certificates, maintains a registry of public keys, and maintains an up-to-date Certificate Revocation List.

§ 1311.05 Standards for technologies for electronic transmission of orders.

(a) A registrant or a person with power of attorney to sign orders for Schedule I and II controlled substances may use any technology to sign and electronically transmit orders if the technology provides all of the following:

(1) *Authentication:* The system must enable a recipient to positively verify the signer without direct communication with the signer and subsequently demonstrate to a third party, if needed, that the sender's identity was properly verified.

(2) *Nonrepudiation:* The system must ensure that strong and substantial evidence is available to the recipient of the sender's identity, sufficient to prevent the sender from successfully denying having sent the data. This criterion includes the ability of a third party to verify the origin of the document.

(3) *Message integrity:* The system must ensure that the recipient, or a third party, can determine whether the contents of the document have been altered during transmission or after receipt.

(b) DEA has identified the following means of electronically signing and transmitting order forms as meeting all of the standards set forth in paragraph (a) of this section.

(1) Digital signatures using Public Key Infrastructure (PKI) technology.

(2) [Reserved]

§ 1311.08 Incorporation by reference.

(a) The following standards are incorporated by reference:

(1) FIPS 140–2, Security Requirements for Cryptographic Modules, May 25, 2001, as amended by Change Notices 2 through 4, December 3, 2002.

(i) Annex A: Approved Security Functions for FIPS PUB 140–2, Security Requirements for Cryptographic Modules, September 23, 2004.

(ii) Annex B: Approved Protection Profiles for FIPS PUB 140–2, Security Requirements for Cryptographic Modules, November 4, 2004.

(iii) Annex C: Approved Random Number Generators for FIPS PUB 140–2, Security Requirements for Cryptographic Modules, January 31, 2005.

(iv) Annex D: Approved Key Establishment Techniques for FIPS PUB 140–2, Security Requirements for Cryptographic Modules, February 23, 2004.

(2) FIPS 180–2, Secure Hash Standard, August 1, 2002, as amended by change notice 1, February 25, 2004.

(3) FIPS 186–2, Digital Signature Standard, January 27, 2000, as amended by Change Notice 1, October 5, 2001.

(b) These standards are available from the National Institute of Standards and Technology, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, 100 Bureau Drive, Gaithersburg, MD 20899–8930 and are available at *http://csrc.nist.gov/.*

(c) These incorporations by reference were approved by the Director of the Federal Register in accordance with 5 U.S.C. 552(a) and 1 CFR part 51. Copies may be inspected at the Drug Enforcement Administration, 600 Army Navy Drive, Arlington, VA 22202 or at the National Archives and Records Administration (NARA). For information on the availability of this material at NARA, call (202) 741–6030, or go to: *http://www.archives.gov/federal_register/code_of_federal_regulations/ibr_locations.html.*

Subpart B—Obtaining and Using Digital Certificates for Electronic Orders

§ 1311.10 Eligibility to obtain a CSOS digital certificate.

The following persons are eligible to obtain a CSOS digital certificate from the DEA Certification Authority to sign electronic orders for controlled substances.

(a) The person who signed the most recent DEA registration application or renewal application and a person authorized to sign a registration application.

(b) A person granted power of attorney by a DEA registrant to sign orders for one or more schedules of controlled substances.

§ 1311.15 Limitations on CSOS digital certificates.

(a) A CSOS digital certificate issued by the DEA Certification Authority will authorize the certificate holder to sign orders for only those schedules of controlled substances covered by the registration under which the certificate is issued.

(b) When a registrant, in a power of attorney letter, limits a certificate applicant to a subset of the registrant's authorized schedules, the registrant is responsible for ensuring that the certificate holder signs orders only for that subset of schedules.

§ 1311.20 Coordinators for CSOS digital certificate holders.

(a) Each registrant, regardless of number of digital certificates issued, must designate one or more responsible persons to serve as that registrant's CSOS coordinator regarding issues pertaining to issuance of, revocation of, and changes to digital certificates issued under that registrant's DEA registration. While the coordinator will be the main point of contact between one or more DEA registered locations and the CSOS Certification Authority, all digital certificate activities are the responsibility of the registrant with whom the digital certificate is associated. Even when an individual registrant, *i.e.*, an individual practitioner, is applying for a digital certificate to order controlled substances a CSOS Coordinator must be designated; though in such a case, the individual practitioner may also serve as the coordinator.

(b) Once designated, coordinators must identify themselves, on a one-time basis, to the Certification Authority. If a designated coordinator changes, the Certification Authority must be notified of the change and the new responsibilities assumed by each of the registrant's coordinators, if applicable. Coordinators must complete the application that the DEA Certification Authority provides and submit the following:

(1) Two copies of identification, one of which must be a government-issued photographic identification.

(2) A copy of each current DEA Certificate of Registration (DEA form 223) for each registered location for which the coordinator will be responsible or, if the applicant (or their employer) has not been issued a DEA registration, a copy of each application for registration of the applicant or the applicant's employer.

(3) The applicant must have the completed application notarized and forward the completed application and accompanying documentation to the DEA Certification Authority.

(c) Coordinators will communicate with the Certification Authority regarding digital certificate applications, renewals and revocations. For applicants applying for a digital certificate from the DEA Certification Authority, and for applicants applying for a power of attorney digital certificate for a DEA registrant, the registrant's Coordinator must verify the applicant's identity, review the application package, and submit the completed package to the Certification Authority.

§ 1311.25 Requirements for obtaining a CSOS digital certificate.

(a) To obtain a certificate to use for signing electronic orders for controlled substances, a registrant or person with power of attorney for a registrant must complete the application that the DEA Certification Authority provides and submit the following:

(1) Two copies of identification, one of which must be a government-issued photographic identification.

(2) A current listing of DEA registrations for which the individual has authority to sign controlled substances orders.

(3) A copy of the power of attorney from the registrant, if applicable.

(4) An acknowledgment that the applicant has read and understands the Subscriber Agreement and agrees to the statement of subscriber obligations that DEA provides.

(b) The applicant must provide the completed application to the registrant's coordinator for CSOS digital certificate holders who will review the application and submit the completed application and accompanying documentation to the DEA Certification Authority.

(c) When the Certification Authority approves the application, it will send the applicant a one-time use reference number and access code, via separate channels, and information on how to use them. Using this information, the applicant must then electronically submit a request for certification of the public digital signature key. After the request is approved, the Certification Authority will provide the applicant with the signed public key certificate.

(d) Once the applicant has generated the key pair, the Certification Authority must prove that the user has possession of the key. For public keys, the corresponding private key must be used to sign the certificate request. Verification of the signature using the public key in the request will serve as proof of possession of the private key.

§ 1311.30 Requirements for storing and using a private key for digitally signing orders.

(a) Only the certificate holder may access or use his or her digital certificate and private key.

(b) The certificate holder must provide FIPS-approved secure storage for the private key, as discussed by FIPS 140–2, 180–2, 186–2, and accompanying change notices and annexes, as incorporated by reference in § 1311.08.

(c) A certificate holder must ensure that no one else uses the private key. While the private key is activated, the certificate holder must prevent unauthorized use of that private key.

(d) A certificate holder must not make back-up copies of the private key.

(e) The certificate holder must report the loss, theft, or compromise of the private key or the password, via a revocation request, to the Certification Authority within 24 hours of substantiation of the loss, theft, or compromise. Upon receipt and verification of a signed revocation request, the Certification Authority will revoke the certificate. The certificate holder must apply for a new certificate under the requirements of § 1311.25.

§ 1311.35 Number of CSOS digital certificates needed.

A purchaser of Schedule I and II controlled substances must obtain a separate CSOS certificate for each registered location for which the purchaser will order these controlled substances.

§ 1311.40 Renewal of CSOS digital certificates.

(a) A CSOS certificate holder must generate a new key pair and obtain a new CSOS digital certificate when the registrant's DEA registration expires or whenever the information on which the certificate is based changes. This information includes the registered name and address, the subscriber's name, and the schedules the registrant is authorized to handle. A CSOS certificate will expire on the date on which the DEA registration on which the certificate is based expires.

(b) The Certification Authority will notify each CSOS certificate holder 45 days in advance of the expiration of the certificate holder's CSOS digital certificate.

(c) If a CSOS certificate holder applies for a renewal before the certificate expires, the certificate holder may renew electronically twice. For every third renewal, the CSOS certificate holder must submit a new application and documentation, as provided in § 1311.25.

(d) If a CSOS certificate expires before the holder applies for a renewal, the certificate holder must submit a new application and documentation, as provided in § 1311.25.

§ 1311.45 Requirements for registrants that allow powers of attorney to obtain CSOS digital certificates under their DEA registration.

(a) A registrant that grants power of attorney must report to the DEA Certification Authority within 6 hours of either of the following (advance notice may be provided, where applicable):

(1) The person with power of attorney has left the employ of the institution.

(2) The person with power of attorney has had his or her privileges revoked.

(b) A registrant must maintain a record that lists each person granted power of attorney to sign controlled substances orders.

§ 1311.50 Requirements for recipients of digitally signed orders.

(a) The recipient of a digitally signed order must do the following before filling the order:

(1) Verify the integrity of the signature and the order by having the system validate the order.

(2) Verify that the certificate holder's CSOS digital certificate has not expired by checking the expiration date against the date the order was signed.

(3) Check the validity of the certificate holder's certificate by checking the Certificate Revocation List.

(4) Check the certificate extension data to determine whether the sender has the authority to order the controlled substance.

(b) A recipient may cache Certificate Revocation Lists for use until they expire.

§ 1311.55 Requirements for systems used to process digitally signed orders.

(a) A CSOS certificate holder and recipient of an electronic order may use any system to write, track, or maintain orders provided that the system has been enabled to process digitally signed documents and that it meets the requirements of paragraph (b) or (c) of this section.

(b) A system used to digitally sign Schedule I or II orders must meet the following requirements:

(1) The cryptographic module must be FIPS 140–2, Level 1 validated, as incorporated by reference in § 1311.08.

(2) The digital signature system and hash function must be compliant with FIPS 186–2 and FIPS 180–2, as incorporated by reference in § 1311.08.

(3) The private key must be stored on a FIPS 140–2 Level 1 validated cryptographic module using a FIPS-approved encryption algorithm, as incorporated by reference in § 1311.08.

(4) The system must use either a user identification and password combination or biometric authentication to access the private key. Activation data must not be displayed as they are entered.

(5) The system must set a 10-minute inactivity time period after which the certificate holder must reauthenticate the password to access the private key.

(6) For software implementations, when the signing module is deactivated, the system must clear the plain text private key from the system memory to prevent the unauthorized access to, or use of, the private key.

(7) The system must be able to digitally sign and transmit an order.

(8) The system must have a time system that is within five minutes of the official National Institute of Standards and Technology time source.

(9) The system must archive the digitally signed orders and any other records required in part 1305 of this chapter, including any linked data.

(10) The system must create an order that includes all data fields listed under § 1305.21(b) of this chapter.

(c) A system used to receive, verify, and create linked records for orders signed with a CSOS digital certificate must meet the following requirements:

(1) The cryptographic module must be FIPS 140–2, Level 1 validated, as incorporated by reference in § 1311.08.

(2) The digital signature system and hash function must be compliant with FIPS 186–2 and FIPS 180–2, as incorporated by reference in § 1311.08.

(3) The system must determine that an order has not been altered during transmission. The system must invalidate any order that has been altered.

(4) The system must validate the digital signature using the signer's public key. The system must invalidate any order in which the digital signature cannot be validated.

(5) The system must validate that the DEA registration number contained in the body of the order corresponds to the registration number associated with the specific certificate by separately generating the hash value of the registration number and certificate subject distinguished name serial number and comparing that hash value to the hash value contained in the certificate extension for the DEA registration number. If the hash values are not equal the system must invalidate the order.

(6) The system must check the Certificate Revocation List automatically and invalidate any order with a certificate listed on the Certificate Revocation List.

(7) The system must check the validity of the certificate and the Certification Authority certificate and invalidate any order that fails these validity checks.

(8) The system must have a time system that is within five minutes of the official National Institute of Standards and Technology time source.

(9) The system must check the substances ordered against the schedules that the registrant is allowed to order and invalidate any order that includes substances the registrant is not allowed to order.

(10) The system must ensure that an invalid finding cannot be bypassed or ignored and the order filled.

(11) The system must archive the order and associate with it the digital certificate received with the order.

(12) If a registrant sends reports on orders to DEA, the system must create a report in the format DEA specifies, as provided in § 1305.29 of this chapter.

(d) For systems used to process CSOS orders, the system developer or vendor must have an initial independent third-party audit of the system and an additional independent third-party audit whenever the signing or verifying functionality is changed to determine whether it correctly performs the functions listed under paragraphs (b) and (c) of this section. The system developer must retain the most recent audit results and retain the results of any other audits of the software completed within the previous two years.

§ 1311.60 Recordkeeping.

(a) A supplier and purchaser must maintain records of CSOS electronic orders and any linked records for two years. Records may be maintained electronically. Records regarding controlled substances that are maintained electronically must be readily retrievable from all other records.

(b) Electronic records must be easily readable or easily rendered into a format that a person can read. They must be made available to the Administration upon request.

(c) CSOS certificate holders must maintain a copy of the subscriber agreement that the Certification Authority provides for the life of the certificate.

PART 1312—IMPORTATION AND EXPORTATION OF CONTROLLED SUBSTANCES

Sec.
1312.01 Scope of part 1312.
1312.02 Definitions.

IMPORTATION OF CONTROLLED SUBSTANCES

1312.11 Requirement of authorization to import.
1312.12 Application for import permit.
1312.13 Issuance of import permit.
1312.14 Distribution of copies of import permit.
1312.15 Shipments in greater or less amount than authorized.
1312.16 Cancellation of permit; expiration date.
1312.17 Special report from importers.
1312.18 Contents of import declaration.
1312.19 Distribution of import declaration.

EXPORTATION OF CONTROLLED SUBSTANCES

1312.21 Requirement of authorization to export.
1312.22 Application for export permit.
1312.23 Issuance of export permit.
1312.24 Distribution of copies of export permit.
1312.25 Expiration date.
1312.26 Records required of exporter.
1312.27 Contents of special controlled substances invoice.
1312.28 Distribution of special controlled substances invoice.
1312.29 Domestic release prohibited.
1312.30 Schedule III, IV, and V non-narcotic controlled substances requiring an import and export permit.

TRANSSHIPMENT AND IN-TRANSIT SHIPMENT OF CONTROLLED SUBSTANCES

1312.31 Schedule I: Application for prior written approval.
1312.32 Schedules II, III, IV: Advance notice.

HEARINGS

1312.41 Hearings generally.
1312.42 Purpose of hearing.
1312.43 Waiver or modification of rules.
1312.44 Request for hearing or appearance; waiver.
1312.45 Burden of proof.
1312.46 Time and place of hearing.
1312.47 Final order.

AUTHORITY: 21 U.S.C. 952, 953, 954, 957, 958.

SOURCE: 36 FR 7815, Apr. 24, 1971, unless otherwise noted. Redesignated at 38 FR 26609, Sept. 24, 1973.